

Enumerative Coding for Line Polar Grassmannians with applications to codes

Ilaria Cardinali* and Luca Giuzzi[†]

March 3, 2016

Abstract

A k -polar Grassmannian is the geometry having as pointset the set of all k -dimensional subspaces of a vector space V which are totally isotropic for a given non-degenerate bilinear form μ defined on V . Hence it can be regarded as a subgeometry of the ordinary k -Grassmannian. In this paper we deal with orthogonal line Grassmannians and with symplectic line Grassmannians, i.e. we assume $k = 2$ and μ a non-degenerate symmetric or alternating form. We will provide a method to efficiently enumerate the pointsets of both orthogonal and symplectic line Grassmannians. This has several nice applications; among them, we shall discuss an efficient encoding/decoding/error correction strategy for line polar Grassmann codes of both types.

Keywords: Enumerative Coding, Polar Grassmannian, Linear Code

MSC: 14M15, 94B27, 94B05.

1 Introduction

Let V be a vector space of dimension n over a field \mathbb{K} . For any $k < n$, the k -Grassmannian $\mathcal{G}_{n,k}$ of V is the geometry whose pointset $\mathcal{P}(\mathcal{G}_{n,k})$ consists of k -dimensional subspaces of V and whose lines are sets of the form

$$\ell_{X,Y} := \{Z : X < Z < Y : \dim z = k\}$$

where X and Y are two subspaces of V with $\dim(X) = k - 1$ and $\dim(Y) = k + 1$. Incidence is containment. It is well known that $\mathcal{G}_{n,k}$ can be embedded, as an algebraic variety, into the projective space $\text{PG}(W)$, where $W = \bigwedge^k V$, by means of the Plücker embedding ε_k ; see [13, Chapter VII] and [14, Chapter XVI] for details.

It is well known that the k -Grassmannian of a n -dimensional vector space over a finite field $\mathbb{K} = \mathbb{F}_q$ has $N := \begin{bmatrix} n \\ k \end{bmatrix}_q$ points. A basic problem is to construct an enumerator for the points of $\mathcal{G}_{n,k}$, that is a bijection $\iota : \{0, 1, \dots, N - 1\} \rightarrow \mathcal{P}(\mathcal{G}_{n,k})$. This has been studied extensively, see [26], because of its relevance to applications. In particular, Grassmannians defined over finite fields have applications in coding theory, for both linear projective codes [23, 24] and network codes [17]. Observe that it is not convenient to attempt to implement a Grassmann code by

*I. Cardinali is with Department of Information Engineering and Mathematics, University of Siena, Via Roma 56, I-53100, Siena, Italy e-mail: ilaria.cardinali@unisi.it

[†]Luca Giuzzi is with DICATAM — Section of Mathematics, University of Brescia, Via Branze 43, I-25123, Brescia, Italy e-mail: luca.giuzzi@unibs.it.

naïvely providing generator matrix, as the number N of columns is fairly large; actually, it is necessary to directly compute the value of any fixed component in an independent way. An enumerator ι provides a unique way to identify the subspace corresponding to a given position. To this purpose, some algorithms for enumerating the points of Grassmannians have been proposed; see [26, 19]. We point out that, apart from their usefulness for applications, these algorithms also have independent geometric interest.

The present paper is concerned with the problem outlined above, focusing on the case of line polar Grassmannians. These are proper subgeometries of line Grassmannians representing the set of lines of a vector space V which are totally isotropic for a given non-degenerate symmetric or alternating form. We shall determine a method to enumerate such lines, following the basic approach of [7]. In general, the case of polar Grassmannians appears more involved than that of ordinary ones, as there are some requirements imposed on the subspaces which have to be fulfilled; thus, a careful use of linear algebra (combined with combinatorial techniques) is necessary in order to get a reasonably efficient representation. We shall also examine in detail the computational complexity of the proposed algorithms.

Our algorithms will be applied to polar Grassmann codes of orthogonal and symplectic type. Such codes have been introduced in [2] and in [3] as linear codes arising from the Plücker embedding of polar Grassmannians of orthogonal or symplectic type respectively. In both cases, some bounds on the minimum distance have been obtained. In particular, in the case $k = 2$ and q odd, the minimum distance of a line orthogonal Grassman code has been proved in [4] to be $q^{4n-5} - q^{3n-4}$, while the minimum distance of a line symplectic Grassman code is $q^{4n-5} - q^{2n-3}$ (see [3]).

In Section 1.1 we shall set the notation and in Section 1.2 introduce polar Grassmann codes. The organization of the paper and the Main results are outlined in Section 1.3.

1.1 Notation

Let $V := V(2n + 1, q)$ be a vector space of dimension $2n + 1$ over a finite field \mathbb{F}_q and let $\mathbf{q}_n : V \rightarrow \mathbb{F}_q$ be a non-degenerate quadratic form. For $q = 2^s$ denote by $\text{Tr}_2(x)$ the absolute trace of $x \in \mathbb{F}_q$, that is to say

$$\text{Tr}_2(x) := \sum_{i=0}^{s-1} x^{2^i}.$$

The k -orthogonal Grassmannian $\Delta_{n,k}$ is a point-line geometry whose points W are all the totally \mathbf{q}_n -singular k -subspaces of V and whose lines are sets either of the form

$$\ell_{X,Z} := \{Y \in \mathcal{G}_{2n+1,k} : X < Y < Z\}$$

where $\dim X = k - 1$, $\dim Z = k + 1$ and Z is totally \mathbf{q}_n -singular for $k < n$ or of the form

$$\ell_X := \{Y : X < Y < X^{\perp \mathbf{q}}, \dim Y = n, Y \text{ totally singular}\},$$

with $\dim X = n - 1$ when $k = n$ and $X^{\perp \mathbf{q}}$ denotes the space orthogonal to X with respect to the bilinear form \mathbf{b}_n associated to \mathbf{q}_n . Incidence is defined in the natural way.

Likewise, denote by $\overline{V} := V(2n, q)$ a vector space of dimension $2n$ over a finite field \mathbb{F}_q and consider a non-degenerate alternating bilinear form $\mathfrak{s} : V \times V \rightarrow \mathbb{F}_q$. The k -Symplectic Grassmannian $\overline{\Delta}_{n,k}$ has as points all totally \mathfrak{s} -isotropic k -spaces W and as lines the sets of the form

$$\ell_{X,Z} = \{Y \in \mathcal{G}_{2n,k} : X < Y < Z\}$$

with $\dim X = k - 1$, $\dim Z = k + 1$ and Z totally \mathfrak{s} -isotropic for $k < n$ and

$$\ell_X = \{Y : X < Y, \dim Y = n, Y \text{ totally isotropic}\}$$

with $\dim X = n - 1$, for $k = n$.

By construction, any point of $\Delta_{n,k}$ is also a point of $\mathcal{G}_{2n+1,k}$, while any point of $\overline{\Delta}_{n,k}$ is a point of $\mathcal{G}_{2n,k}$.

It is well known that the Plücker embedding e_k which associates to a k -vector subspace $X = \langle v_1, v_2, \dots, v_k \rangle$ of V the point $[v_1 \wedge v_2 \wedge \dots \wedge v_k]$ of $\text{PG}(\bigwedge^k V)$ is a projective embedding of the Grassmannian. That is, e_k is injective and each line of the Grassmannian \mathcal{G}_k is mapped onto a line of $\mathbb{G}_k := e_k(\mathcal{G}_k)$. Furthermore \mathbb{G}_k is an algebraic variety of $\text{PG}(\bigwedge^k V)$ and also $\langle \mathbb{G}_k \rangle = \bigwedge^k V$.

We can consider the embedding ε_k of the polar Grassmannians of orthogonal and symplectic type induced by e_k . In particular, $\varepsilon_k(\Delta_{n,k})$ is a subvariety of $\mathbb{G}_{2n+1,k}$ and $\overline{\varepsilon}_k(\overline{\Delta}_{n,k})$ is a subvariety of $\mathbb{G}_{2n,k}$.

We summarize what is known about these embeddings. We warn the reader that we shall always use vector dimensions.

Theorem 1 ([5]). *Let $\varepsilon_k : \Delta_{n,k} \rightarrow \text{PG}(\bigwedge^k V)$ be the restriction of the Plücker embedding to the orthogonal polar Grassmannian $\Delta_{n,k}$ and let $W_{n,k} := \langle \varepsilon_k(\Delta_{n,k}) \rangle$. Then,*

- For $k < n$, ε_k is projective and

$$\dim W_{n,k} = \begin{cases} \binom{2n+1}{k} & \text{if } \text{char}(\mathbb{F}) \text{ odd} \\ \binom{2n+1}{k} - \binom{2n+1}{k-2} & \text{if } \text{char}(\mathbb{F}) = 2 \end{cases}$$

- For $k = n$, $\varepsilon_n : \Delta_{n,n} \rightarrow \text{PG}(W_{n,n})$ maps lines into conics.

Theorem 2 ([8, 21]). *Let $\overline{\varepsilon}_k : \overline{\Delta}_{n,k} \rightarrow \text{PG}(\bigwedge^k V)$ be the restriction of the Plücker embedding to the symplectic polar Grassmannian $\overline{\Delta}_{n,k}$ and let $\overline{W}_{n,k} := \langle \overline{\varepsilon}_k(\overline{\Delta}_{n,k}) \rangle$. Then,*

- $\overline{\varepsilon}_k : \overline{\Delta}_{n,k} \rightarrow \text{PG}(\bigwedge^k V)$ is projective and $\dim(\overline{W}_{n,k}) = \binom{2n}{k} - \binom{2n}{k-2}$.

1.2 Polar Grassmann Codes

In order to avoid confusion, we shall denote throughout the paper by N the length of a linear code and by K its dimension; as before, lower case letters n and k shall be used to represent the parameters of the associated Grassmannians.

A q -ary code \mathcal{C} of length N and dimension K is called *projective* if the columns of its generator matrix are coordinates of N distinct points in $\text{PG}(K - 1, q)$. Conversely, given a set of N distinct points $\Omega = \{P_1, \dots, P_N\}$ in $\text{PG}(W)$, with $\dim W = K$ we call *projective code induced by Ω* any linear code $\mathcal{C}(\Omega)$ having a generator matrix G whose columns consists of coordinates of the points in Ω with respect to some reference. Clearly, $\mathcal{C}(\Omega)$ is defined only up to code equivalence, but in the remaining of this paper we shall speak, with a slight abuse of notation, of *the* code induced by Ω ; see [27] for more details.

A basic result in the theory of projective codes shows that there is a close link between hyperplane sections of Ω and weights of the codewords of $\mathcal{C}(\Omega)$. In particular, hyperplanes of $\text{PG}(W)$ having maximal intersection with Ω are associated with codewords of minimum weight.

The projective codes $\mathcal{C}_{n,k}$ arising from the pointset $e_k(\mathcal{G}_{n,k}) \subseteq \text{PG}(\bigwedge^k V)$ are called Grassmann codes. They have been introduced in [23, 24] as a generalization of Reed-Muller codes of the first

order and have been widely investigated ever since: both their monomial automorphism groups and minimum weights are well understood, see [10, 11, 12, 15, 20, 25]. These codes have a fairly low rate; as such, in order to have an efficient implementation, it is paramount to provide efficient encoding and decoding algorithms, acting locally on the components. To this aim, in [26] an enumerative coding scheme for Grassmannians is considered and some efficient algorithms are presented; see also [19].

Starting with [2] we have been considering linear codes arising from the Plücker embedding of polar Grassmannians of either orthogonal or symplectic type. In particular, in [2] a new family of linear codes related to the Plücker embedding of polar Orthogonal Grassmannians $\Delta_{n,k}$ has been introduced and some bound on its minimum distance have been determined.

In close analogy to orthogonal Grassmann codes we defined in [3] Symplectic Grassmann codes, that is codes arising from the Plücker embedding of the symplectic Grassmannian $\overline{\Delta}_{n,k}$.

Either family of polar Grassmann codes can be obtained from the ordinary Grassmann codes $\mathcal{C}_{2n+1,k}$ or $\mathcal{C}_{2n,k}$ by just deleting all the columns corresponding respectively to k -spaces which are non-singular with respect to \mathfrak{q}_n or non-isotropic with respect to \mathfrak{s} — as such they can be regarded in a natural way as punctured versions of $\mathcal{C}_{2n+1,k}$ or $\mathcal{C}_{2n,k}$. We summarize in the following theorems what is currently known about the parameters of these codes.

Theorem 3 ([2],[4]). *The known parameters $[N, K, d]$ of $\mathcal{P}_{n,k} := \mathcal{C}(\Delta_{n,k})$ are*

(n, k)	N	K	d	Reference
$1 \leq k < n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)} - 1}{q^{i+1} - 1}$	$\binom{2n+1}{k}$	$d \geq \tilde{d}(q, n, k)$	[2]
$(3, 3)$	$(q^3 + 1)(q^2 + 1)(q + 1)$	35	$q^2(q - 1)(q^3 - 1)$	[2]
$(n, 2)$	$\frac{(q^{2n-1} - 1)(q^{2n-2} - 1)}{(q - 1)(q^2 - 1)}$	$(2n + 1)n$	$q^{4n-5} - q^{3n-4}$	[4]

q odd

(n, k)	N	K	d	Reference
$1 \leq k < n$	$\prod_{i=0}^{k-1} \frac{q^{2(n-i)} - 1}{q^{i+1} - 1}$	$\binom{2n+1}{k} - \binom{2n+1}{k-2}$	$d \geq \tilde{d}(q, n, k)$	[2]
$(2, 2)$	$(q^2 + 1)(q + 1)$	9	$q^2(q - 1)$	[2]
$(3, 3)$	$(q^3 + 1)(q^2 + 1)(q + 1)$	28	$q^5(q - 1)$	[2]

q even

$$\tilde{d}(q, n, k) := (q + 1)(q^{k(n-k)} - 1) + 1$$

Theorem 4 ([3]). *The known parameters $[N, K, d]$ of $\mathcal{W}_{n,k} := \mathcal{C}(\overline{\Delta}_{n,k})$ are*

(n, k)	N	K	d	Reference
$1 < k \leq n$	$\prod_{i=0}^{k-1} (q^{2n-2i} - 1) / (q^{i+1} - 1)$	$\binom{2n}{k} - \binom{2n}{k-2}$		[3]
$(n, 2)$	$\frac{(q^{2n-1} - 1)(q^{2n-2} - 1)}{(q - 1)(q^2 - 1)}$	$n(2n - 1) - 1$	$q^{4n-5} - q^{2n-3}$	[3]
$(3, 3)$	$(q^3 + 1)(q^2 + 1)(q + 1)$	14	$q^6 - q^4$	[3]

1.3 Organization of the paper and Main Results

The structure of the paper is as follows. In Section 2 we recall the notion of prefix enumeration and describe counting algorithms for the pointsets of both $\Delta_{n,2}$ and $\overline{\Delta}_{n,2}$. In particular, in 2.2 we consider the number of totally singular lines of V for \mathbf{q}_n , spanned by vectors with a prescribed prefix, while in 2.3 we investigate the totally isotropic lines of \overline{V} for \mathbf{s} .

These results are used in Section 3 to present an enumerative coding scheme according to the approach of [7]; In 2.2.3 we analyze the overall complexity of our enumerative encoding scheme.

It will be apparent that our analysis in the orthogonal case must be more involved than that of [26] for Grassmann codes; consequently the complexity of the algorithm changes.

Theorem 5. *The computational complexity of the enumerative algorithm for orthogonal line grassmannians is $O(n^2)$. The computational complexity of the enumerative algorithm for symplectic line grassmannians is $O(n)$.*

Section 4 is dedicated to applications of the scheme introduced in Section 3 to polar Grassmann codes. We also propose some encoding/decoding and error correction strategies which act locally on the components of the codewords.

2 Prefix enumeration

In this section we shall present an algorithm to count the points of a line polar Grassmannian. This will be essential for the enumerative encoding algorithm of Section 3.

2.1 Preliminaries

In order to simplify the exposition, in this section we shall slightly alter the notation introduced in Section 1.1. For $\varepsilon = 0, 1$, let $V^\varepsilon := V(2n + \varepsilon, q)$ be a vector space of dimension $2n + \varepsilon$ over \mathbb{F}_q and let \mathfrak{B}_ε a fixed basis of V^ε . So, according to Section 1.1, $V^0 := \overline{V}$ and $V^1 := V$. Up to projectivities, there is exactly one class of non-degenerate quadratic forms on V^1 ; hence, it is not restrictive to fix the following quadratic form \mathbf{q}_n :

$$\mathbf{q}_n(\mathbf{x}) = x_1^2 + \sum_{i=1}^n x_{2i}x_{2i+1}, \quad (1)$$

where $x = (x_i)_{i=1}^{2n+1}$. The associated bilinear form \mathbf{b}_n is

$$\mathbf{b}_n(x, y) := 2x_1y_1 + \sum_{i=1}^n (x_{2i}y_{2i+1} + y_{2i}x_{2i+1}),$$

where $x = (x_i)_{i=1}^{2n+1}$, $y = (y_i)_{i=1}^{2n+1}$. Note that, for q even, the form \mathbf{b}_n is alternating and degenerate, while for q odd \mathbf{b}_n is non-degenerate and symmetric.

If $\varepsilon = 0$, consider the following non-degenerate symplectic form $\mathbf{s} : \overline{V} \times \overline{V} \rightarrow \mathbb{F}_q$,

$$\mathbf{s}(x, y) = \sum_{i=1}^n x_{2i-1}y_{2i} - y_{2i-1}x_{2i} \quad (2)$$

where $x = (x_i)_{i=1}^{2n}$, $y = (y_i)_{i=1}^{2n}$.

We recall that a $2 \times t$ matrix G is said to be in Hermite normal form or in *row reduced echelon form* (RREF, in brief) if it is in row-echelon form, the leading non-zero entry of each row is 1

Table 1: Useful numbers

Ξ	# of points of Ξ	# of lines of Ξ
$\text{PG}(v, q)$	$\frac{(q^{v+1}-1)}{q-1}$	$\frac{(q^v-1)(q^{v+1}-1)}{(q^2-1)(q-1)}$
$Q(2v, q)$	$\frac{(q^{2v}-1)}{q-1}$	$\frac{(q^{2v-1}-1)(q^{2v}-1)}{(q^2-1)(q-1)}$
$Q^+(2v-1, q)$	$\frac{(q^v-1)(q^{v-1}+1)}{q-1}$	$\frac{(q^{2v-2}-1)(q^v-1)(q^{v-1}+1)}{(q^2-1)(q-1)}$
$W(2v-1, q)$	$\frac{q^{2v}-1}{q-1}$	$\frac{(q^{2v-1}-1)(q^{2v-2}-1)}{(q-1)(q^2-1)}$

and all entries above a leading entry are 0. For each line $\ell = \langle X, Y \rangle$ of $\text{PG}(V^\epsilon)$ we can choose X and Y such that $G_\ell := \begin{pmatrix} X \\ Y \end{pmatrix}$ is a $2 \times (2n + \epsilon)$ -matrix in RREF and this choice is unique. We call G_ℓ the *representation* of ℓ .

We remind that a line $\ell = \langle X, Y, \rangle$ of $\text{PG}(V^0)$ is said to be *totally \mathfrak{q} -singular* if $\mathfrak{q}_n(X) = \mathfrak{q}_n(Y) = 0 = \mathfrak{b}_n(X, Y)$. Likewise, a line $\ell = \langle X, Y \rangle$ of $\text{PG}(V^1)$ is *totally \mathfrak{s} -isotropic* if $\mathfrak{s}(X, Y) = 0$.

Denote by $\mathcal{M}_{2,t}$ the set of all $2 \times t$ matrices over \mathbb{F}_q and also let

$$\mathcal{M}_2^\epsilon := \bigcup_{i=0}^{2n+\epsilon} \mathcal{M}_{2,i}.$$

with $\epsilon \in \{0, 1\}$ and $\mathcal{M}_{2,0} := \{\emptyset\}$.

Let $S = \begin{pmatrix} \alpha_1 & \dots & \alpha_t \\ \beta_1 & \dots & \beta_t \end{pmatrix} \in \mathcal{M}_2^\epsilon$ and $\begin{matrix} \hat{A} := (\alpha_1, \alpha_2, \dots, \alpha_t, x_{t+1}, x_{t+2}, \dots, x_{2n+\epsilon}) \\ \hat{B} := (\beta_1, \beta_2, \dots, \beta_t, y_{t+1}, y_{t+2}, \dots, y_{2n+\epsilon}) \end{matrix}$.

Then we say that S is the *prefix* or the *leading part* of the $2 \times (2n + 1)$ matrix $\begin{pmatrix} \hat{A} \\ \hat{B} \end{pmatrix}$.

We shall also put $A := (\alpha_1, \alpha_2, \dots, \alpha_t, 0, 0, \dots, 0)$, $B := (\beta_1, \beta_2, \dots, \beta_t, 0, 0, \dots, 0)$.

Definition 1. Let $n_{\mathfrak{q}} : \mathcal{M}_2^1 \times \mathbb{N} \rightarrow \mathbb{N}$ be the function such that for any $S \in \mathcal{M}_2^1$ and $n \in \mathbb{N}$, $n_{\mathfrak{q}}(S, n)$ is the number of totally \mathfrak{q} -singular lines of $\text{PG}(V)$ whose representation (in RREF) has prefix S .

Let $n_{\mathfrak{s}} : \mathcal{M}_2^0 \times \mathbb{N} \rightarrow \mathbb{N}$ be the function such that for any $S \in \mathcal{M}_2^0$ and $n \in \mathbb{N}$, $n_{\mathfrak{s}}(S, n)$ is the number of totally \mathfrak{s} -isotropic lines of $\text{PG}(\overline{V})$ whose representation (in RREF) has prefix S .

It is straightforward to see that $n_{\mathfrak{q}}(S, n) = 0$ and $n_{\mathfrak{s}}(S, n) = 0$ if S is not in RREF. Henceforth, we shall always silently assume that S is given in RREF.

Definition 2. We say that a $2 \times t$ -matrix

$$S = \begin{pmatrix} \alpha_1 & \dots & \alpha_t \\ \beta_1 & \dots & \beta_t \end{pmatrix}$$

is in *close to RREF* (in brief CRREF) if it is in row-echelon form, the leading non-zero entry in each row is 1 and either $\alpha_t = 0$ or $\beta_t = 0$.

Note than, in general, a matrix in CRREF is not is RREF. Indeed, given a $2 \times t$ matrix S in RREF, if either $\alpha_t = 0$ or $\beta_t = 0$, then S is already also in CRREF; otherwise, when $\beta_t \neq 0$, we

can always subtract from the first row of S the second row multiplied by $\lambda = \alpha_t \beta_t^{-1} (\neq 0)$ to get a new matrix

$$S' = \begin{pmatrix} \alpha_1 - \lambda \beta_1 & \dots & 0 \\ \beta_1 & \dots & \beta_t \end{pmatrix}. \quad (3)$$

2.2 Enumerating orthogonal Grassmannians

In this section we shall compute the enumerating function n_q defined in Definition 1. Let $(S, n) \in \mathcal{M}_2^1 \times \mathbb{N}$ and suppose $S \in \mathcal{M}_{2,t}^1$. The value $n_q(S, n)$ is the number of solutions in the unknowns x_i 's and y_i 's, $i = t+1, \dots, 2n+1$, of the system of quadratic equations

$$\begin{cases} \mathfrak{q}_n(\widehat{A}) = 0 \\ \mathfrak{q}_n(\widehat{B}) = 0 \\ \mathfrak{b}_n(\widehat{A}, \widehat{B}) = 0. \end{cases} \quad (4)$$

The first step of the algorithm is to transform S to CRREF using (3).

We will distinguish two cases, depending on the parity of t . These cases will not be fully independent: as it will be seen, our algorithm for t even requires some computations with some auxiliary prefixes S' of odd length and, likewise, some cases with a prefix of odd length are dealt with by reducing to different cases where the prefix contains an even number of components. In any case, as the analysis shall show, this will not lead to an infinite recursion and will ultimately provide the correct value without explicitly requiring to solve (4).

2.2.1 Even t

If $t = 0$, then we just have to count all the (totally singular) lines of $Q(2n, q)$; thus, $n_q(\emptyset, n) = N$, see Table 1 and we are done.

For $t > 0$ even, we need to compute the number of solutions of the following system

$$\begin{cases} \alpha_1^2 + \sum_{i=1}^{t/2-1} \alpha_{2i} \alpha_{2i+1} + \alpha_t x_{t+1} + \sum_{i=t/2+1}^n x_{2i} x_{2i+1} = 0 \\ \beta_1^2 + \sum_{i=1}^{t/2-1} \beta_{2i} \beta_{2i+1} + \beta_t y_{t+1} + \sum_{i=t/2+1}^n y_{2i} y_{2i+1} = 0 \\ 2\alpha_1 \beta_1 + \alpha_t y_{t+1} + \beta_t x_{t+1} + \sum_{i=1}^{t/2-1} (\alpha_{2i} \beta_{2i+1} + \alpha_{2i+1} \beta_{2i}) + \sum_{i=t/2+1}^n (x_{2i} y_{2i+1} + x_{2i+1} y_{2i}) = 0. \end{cases} \quad (5)$$

We distinguish several cases.

A.1) $\boxed{\alpha_t = 0 \text{ and } \beta_t \neq 0}$. The second and third equations of (5) are respectively linear in y_{t+1} and x_{t+1} . So, for any choice of y_{t+2}, \dots, y_{2n+1} there is exactly one value for y_{t+1} . There are q^{2n-t} possibilities.

Consider now the first equation; it now determines x_{t+1} once x_{t+2}, \dots, x_{2n+1} are given. Hence, we need to study just the first equation, which can be written as

$$\mathfrak{q}_n(A) + \sum_{i=t/2+1}^n x_{2i} x_{2i+1} = 0. \quad (6)$$

We determine the number of solutions of (6).

Observe that, as S is in CRREF, we always have $A = (\alpha_1, \dots, \alpha_{t-1}, 0) \neq \mathbf{0}$; i.e. there is $i < t$ such that $\alpha_i \neq 0$. Since $B = (\beta_1, \dots, \beta_t) \neq \mathbf{0}$, any vector solution of (6) and arbitrary choices of y_{t+2}, \dots, y_{2n+1} give different lines. Call $\widehat{\eta}_0(A)$ the number of solutions of (6). If $\mathbf{q}_n(A) = 0$, then $\widehat{\eta}_0(A)$ is the number of vectors satisfying $\mathbf{q}^+(x_{t+2}, \dots, x_{2n+1}) = 0$ where

$$\mathbf{q}^+(x_{t+2}, \dots, x_{2n+1}) := \sum_{i=t/2+1}^n x_{2i}x_{2i+1}.$$

Clearly $\widehat{\eta}_0(A)$ is the number of vectors contained in a hyperbolic quadric \mathcal{Q}^+ in $\text{PG}(2n - t - 1, q)$.

If $\mathbf{q}_n(A) \neq 0$, then $\widehat{\eta}_0(A)$ is the number vector solutions of

$$\mathbf{q}^+(x_{t+2}, \dots, x_{2n+1}) = -\mathbf{q}_n(A).$$

The points of $\text{PG}(2n - t - 1, q)$ lie in 3-orbits under the action of the orthogonal group $O^+(2n - t, q)$.

For q odd, for half of the points of $\text{PG}(2n - t - 1, q)$ not in \mathcal{Q}^+ , the form \mathbf{q}^+ has the same quadratic character as $-\mathbf{q}_n(A)$; each of these points contributes 2 vector solutions to (5). The points with quadratic character different from that of $-\mathbf{q}_n(A)$ do not contribute any solution. Thus, $\widehat{\eta}_0(A) = \eta_0(\mathbf{q}_n(A))$ where

$$\eta_0(c) := \begin{cases} (q-1) \cdot \frac{(q^{n-t/2}-1)(q^{n-t/2-1}+1)}{q-1} + 1 & \text{if } c = 0 \\ 2 \cdot \frac{1}{2} \left(\frac{q^{2n-t}-1}{q-1} - \frac{(q^{n-t/2}-1)(q^{n-t/2-1}+1)}{q-1} \right) & \text{if } c \neq 0. \end{cases} \quad (7)$$

For q even, an analogous argument, where we consider the absolute trace $\text{Tr}_2(\mathbf{q}_n(A))$ of $\mathbf{q}_n(A)$ instead of its quadratic character leads to exactly the same formula (7).

Finally,

$$n_q(S, n) = \underbrace{\#\{\text{solutions of (6)}\}}_{\text{possibilities for } x_{t+2}, \dots, x_{2n+1}} \times \underbrace{q^{2n-t}}_{\text{possibilities for } y_{t+2}, \dots, y_{2n+1}} = \eta_0(\mathbf{q}_n(A)) \cdot q^{2n-t}.$$

A.2) $\alpha_t \neq 0$ and $\beta_t = 0$. This case is analogous to A.1) with the roles of the first and the second equation reversed. The only difference is for $B = \mathbf{0}$. Indeed,

A.2.1) for $B \neq \mathbf{0}$ and $\beta_t = 0$, we argue exactly as in A.1) and $n_q(S, n) = \eta_0(\mathbf{q}_n(B)) \cdot q^{2n-t}$.

A.2.2) for $B = \mathbf{0}$ we need to count the number of points of the hyperbolic quadric having equation $y_{t+2}y_{t+3} + \dots + y_{2n}y_{2n+1} = 0$. Let $i > t$ be the index of the first non-zero component y_i in \widehat{B} ; the corresponding entry x_i in \widehat{A} must be 0, as $\begin{pmatrix} \widehat{A} \\ \widehat{B} \end{pmatrix}$ is in RREF.

So, there are q^{2n-t-1} possibilities for x_{t+1}, \dots, x_{2n+1} . Thus,

$$n_q(S, n) := \frac{q^{2n-t-1}}{q-1} (q^{n-t/2} - 1)(q^{n-t/2-1} + 1).$$

A.3) $\boxed{\alpha_t = \beta_t = 0.}$ In this case the matrix $G = \begin{pmatrix} \hat{A} \\ \hat{B} \end{pmatrix}$ has the form

$$G = \begin{pmatrix} \alpha_1 & \dots & \alpha_{t-1} & 0 & x_{t+1} & \dots & x_{2n+1} \\ \beta_1 & \dots & \beta_{t-1} & 0 & y_{t+1} & \dots & y_{2n+1} \end{pmatrix}.$$

As the coefficients of x_{t+1} and y_{t+1} are both zero, System (5) is formally the same as the system defined by

$$G' = \begin{pmatrix} \alpha_1 & \dots & \alpha_{t-1} & x_{t+2} & \dots & x_{2n+1} \\ \beta_1 & \dots & \beta_{t-1} & y_{t+2} & \dots & y_{2n+1} \end{pmatrix}.$$

We shall call this new system, where the unknowns x_{t+1} and y_{t+1} have been removed, the “reduced” one. It is straightforward to see that for each solution of the reduced system there are q^2 solutions of (5), being x_{t+1} and y_{t+1} arbitrary. Note that the number of solutions of the reduced system is $n_q(S', n-1)$ where

$$S' := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} \end{pmatrix}.$$

We consider three subcases:

A.3.1) $\boxed{A = B = \mathbf{0}.}$ In this case, $n_q(S, n)$ is the number of lines of a parabolic quadric \mathcal{Q} defined by \mathfrak{q}_n contained in the subspace Π of codimension t described by the equations

$$x_1 = 0, x_2 = 0, \dots, x_t = 0.$$

As $\mathcal{Q}' := \Pi \cap \mathcal{Q}$ is a cone of vertex $W = (\overbrace{0, 0, \dots, 0}^t, 1, 0, \dots, 0)$ and basis the hyperbolic quadric \mathcal{Q}^+ of $\text{PG}(2n-t-1, q)$ with equation

$$\begin{cases} x_1 = x_2 = \dots = x_t = 0 \\ x_{t+2}x_{t+3} + x_{t+4}x_{t+5} + \dots + x_{2n}x_{2n+1} = 0 \end{cases},$$

$n_q(S, n) = \sigma q^2 + \#\mathcal{Q}^+$, where σ is the number of lines of \mathcal{Q}^+ ; see Table 1 for the actual values.

A.3.2) $\boxed{A \neq \mathbf{0} \text{ and } B = \mathbf{0}.}$ In this case, $n_q(S, n) := q^2 n_q(S', n-1) + \sigma_1$, where σ_1 corresponds to the number of solutions of (5) which do not arise from solutions of the reduced system. This happens only if the second row of G' is null, but the second row of G is not. That is,

$$G = \begin{pmatrix} A & 0 & x_{t+2} & \dots & x_{2n+1} \\ \mathbf{0} & 1 & 0 & \dots & 0 \end{pmatrix},$$

with $\mathfrak{q}^+(x_{t+2}, \dots, x_{2n+1}) = -\mathfrak{q}_n(A)$. Thus, $\sigma_1 = \eta_0(\mathfrak{q}_n(A))$, see (7).

A.3.3) $\boxed{A \neq \mathbf{0} \text{ and } B \neq \mathbf{0}.}$ In this case, $n_q(S, n) = q^2 n_q(S', n-1)$ and we apply a recursive argument.

Recall that $A = \mathbf{0}$ and $B \neq \mathbf{0}$ cannot occur as the matrix S is in CRREF.

Computing the value of $n_q(S, n)$ when $(\alpha_t, \beta_t) = (0, 0)$ has thus been reduced to solve the problem of determining $n_q(S', n-1)$, where the length t' of S' is odd and the number of unknowns is $2n-t$.

2.2.2 Odd t

We have to consider the system

$$\begin{cases} \alpha_1^2 + \sum_{i=1}^{(t-1)/2} \alpha_{2i} \alpha_{2i+1} + \sum_{i=(t+1)/2}^n x_{2i} x_{2i+1} = 0 \\ \beta_1^2 + \sum_{i=1}^{(t-1)/2} \beta_{2i} \beta_{2i+1} + \sum_{i=(t+1)/2}^n y_{2i} y_{2i+1} = 0 \\ 2\alpha_1 \beta_1 + \sum_{i=1}^{(t-1)/2} (\alpha_{2i} \beta_{2i+1} + \alpha_{2i+1} \beta_{2i}) + \sum_{i=(t+1)/2}^n (x_{2i} y_{2i+1} + x_{2i+1} y_{2i}) = 0. \end{cases} \quad (8)$$

Following the notation of Section 2.1, let $S = \begin{pmatrix} \alpha_1 & \dots & \alpha_t \\ \beta_1 & \dots & \beta_t \end{pmatrix}$ be in RREF with $A = (\alpha_1, \dots, \alpha_t, 0, \dots, 0)$ and $B = (\beta_1, \dots, \beta_t, 0, \dots, 0)$. The technique we apply to determine $n_q(S, n)$ is to replace S with a larger matrix $S_{\gamma, \delta}$ obtained from S by adding the column $\begin{pmatrix} \gamma \\ \delta \end{pmatrix}$:

$$S_{\gamma, \delta} = \begin{pmatrix} \alpha_1 & \dots & \alpha_t & \gamma \\ \beta_1 & \dots & \beta_t & \delta \end{pmatrix}.$$

We distinguish several cases.

B.1) $\boxed{A \neq \mathbf{0} \text{ and } B \neq \mathbf{0}}$ The sets of lines determined by $S_{\gamma, \delta}$ as γ, δ vary in \mathbb{F}_q are all disjoint; thus,

$$n_q(S, n) = \sum_{(\gamma, \delta) \in \mathbb{F}_q^2} n_q(S_{\gamma, \delta}, n).$$

Hence we need to compute the values $n_q(S_{\gamma, \delta}, n)$ with $S_{\gamma, \delta}$ of even length. More precisely,

$$n_q(S, n) = \Psi_{\substack{\gamma \neq 0 \\ \delta \neq 0}} + \Psi_{\substack{\gamma \neq 0 \\ \delta = 0}} + \Psi_{\substack{\gamma = 0 \\ \delta \neq 0}} + \Psi_{\substack{\gamma = 0 \\ \delta = 0}},$$

where the addends are as follows.

B.1.1) $\boxed{\Psi_{\substack{\gamma \neq 0 \\ \delta \neq 0}}}$ Let $\lambda = \delta^{-1} \gamma$. We have $n_q(S_{\gamma, \delta}, n) = n_q(S', n)$ where

$$S' := \begin{pmatrix} \alpha_1 - \lambda \beta_1 & \dots & \alpha_t - \lambda \beta_t & 0 \\ \beta_1 & \dots & \beta_t & \delta \end{pmatrix}.$$

Since S' has $t+1$ columns, we are lead back to Case A.1) of Subsection 2.2.1. Thus,

$$n_q(S', n) = q^{2n-t-1} \eta_1(c),$$

with $\eta_1(c)$ the number of solutions of the equation $\mathbf{q}_n(A - \lambda B) = 0$, as λ varies in $\mathbb{F}_q \setminus \{0\}$. If $c := \mathbf{q}_n(A - \lambda B)$, then (see also (7))

$$\eta_1(c) := \begin{cases} (q-1) \cdot \frac{(q^{n-(t+1)/2}-1)(q^{n-(t+3)/2}+1)}{q-1} + 1 & \text{if } c = 0 \\ 2 \cdot \frac{1}{2} \left(\frac{q^{2n-t-1}-1}{q-1} - \frac{(q^{n-(t+1)/2}-1)(q^{n-(t+3)/2}+1)}{q-1} \right) & \text{if } c \neq 0. \end{cases} \quad (9)$$

Table 2: Number ξ of solutions $\mathbf{q}_n(A) - \lambda \mathbf{b}_n(A, B) + \lambda^2 \mathbf{q}_n(B)$ for q odd

$\mathbf{q}_n(A)$	$\mathbf{b}_n(A, B)$	$\mathbf{q}_n(B)$	Δ	ξ
0	0	0	0	$q - 1$
0	$\neq 0$	$\neq 0$	*	1
0	0	$\neq 0$	0	0
0	$\neq 0$	0	*	0
$\neq 0$	0	0	*	0
$\neq 0$	$\neq 0$	0	*	1
$\neq 0$	Any	$\neq 0$	\square	2
$\neq 0$	Any	$\neq 0$	0	1
$\neq 0$	Any	$\neq 0$	∇	0

$$\Delta := \mathbf{b}_n(A, B)^2 - 4\mathbf{q}_n(A)\mathbf{q}_n(B).$$

* means that there are no conditions on Δ

We have

$$c = \mathbf{q}_n(A) - \lambda \mathbf{b}_n(A, B) + \lambda^2 \mathbf{q}_n(B). \quad (10)$$

Let now ξ be the number of non-zero solutions of (10) in the unknown λ . Then, the possible values assumed by ξ are outlined in Table 2 for q odd and in Table 3 for q even. For q odd, the symbols \square and ∇ represent respectively the set of all non-zero square elements and the set of non-square elements in \mathbb{F}_q . Hence,

$$\Psi_{\substack{\gamma \neq 0 \\ \delta \neq 0}} = \underbrace{(q-1)}_{\text{cases for } \delta} q^{2n-t-1} \left(\underbrace{\xi \eta_1(0)}_{\text{first eq. homogeneous}} + \underbrace{(q-1-\xi) \eta_1(1)}_{\text{first eq. nonhomogeneous}} \right).$$

B.1.2) $\boxed{\Psi_{\substack{\gamma \neq 0 \\ \delta = 0}} \text{ or } \Psi_{\substack{\gamma = 0 \\ \delta \neq 0}}}$ Arguing as in A.1 of Section 2.2.1, we see that $n_q(S_{0,\delta}, n) = n_q(S_{0,1}, n)$ for any $\delta \neq 0$. Hence,

$$\Psi_{\substack{\gamma \neq 0 \\ \delta = 0}} = (q-1)n_q(S_{0,1}, n),$$

where the factor $n_q(S_{0,1}, n)$ can be directly computed as in A.1).

The case $\gamma \neq 0$ and $\delta = 0$ is analogous to case A.2.1; hence,

$$\Psi_{\substack{\gamma = 0 \\ \delta \neq 0}} = (q-1)n_q(S_{1,0}, n).$$

B.1.3) $\boxed{\Psi_{\substack{\gamma = 0 \\ \delta = 0}}}$ In this case $\Psi_{\substack{\gamma = 0 \\ \delta = 0}} = q^2 n_q(S, n-1)$ as x_{t+2} and y_{t+2} may be chosen arbitrarily and $n_q(S, n-1)$ is the number of solutions of the System associated to

$$G = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t & x_{t+3} & \dots & x_{2n+1} \\ \beta_1 & \beta_2 & \dots & \beta_t & y_{t+3} & \dots & y_{2n+1} \end{pmatrix}.$$

B.2) $\boxed{A = B = \mathbf{0}}$ An argument analogous to that of Case A.3.1 of Subsection 2.2.1 shows that we need to determine the number of lines of a hyperbolic quadric \mathcal{Q}^+ in $\text{PG}(2n-t, q)$ with equation

$$x_{t+1}x_{t+2} + \dots + x_{2n}x_{2n+1} = 0;$$

Table 3: Number ξ of solutions $\mathbf{q}_n(A) + \lambda \mathbf{b}_n(A, B) + \lambda^2 \mathbf{q}_n(B)$ for q even

$\mathbf{q}_n(A)$	$\mathbf{b}_n(A, B)$	$\mathbf{q}_n(B)$	Θ	value
0	0	0	*	$q - 1$
0	$\neq 0$	$\neq 0$	*	1
0	0	$\neq 0$	*	0
0	$\neq 0$	0	*	0
$\neq 0$	0	0	*	0
$\neq 0$	$\neq 0$	0	*	1
$\neq 0$	0	$\neq 0$	*	1
$\neq 0$	$\neq 0$	$\neq 0$	0	2
$\neq 0$	$\neq 0$	$\neq 0$	1	0

$$\Theta := \text{Tr}_2 \left(\frac{\mathbf{q}_n(A) \mathbf{q}_n(B)}{\mathbf{b}_n(A, B)^2} \right)$$

* means that there are no conditions on Θ or Θ does not exist.

we refer to Table 1 for the actual value.

B.3) $\boxed{A \neq \mathbf{0} \text{ and } B = \mathbf{0}.}$ In this case we have to consider

$$S_{\gamma, \delta} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t & \gamma \\ 0 & 0 & \dots & 0 & \delta \end{pmatrix}$$

in RREF. In particular, either $\delta = 1$ and $\gamma = 0$ or $\delta = 0$ and γ is arbitrary. Note that for any solution of the first equation of (8) there are $q - 1$ solutions of the second equation yielding the same line.

B.3.1) $\boxed{(\gamma, \delta) = (0, 1)}$ We can directly compute $n_q(S_{0,1}, n)$ using the same approach as in A.1).

B.3.2) $\boxed{\delta = 0 \text{ and } \gamma \neq 0.}$ We have

$$S_{\gamma, 0} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t & \gamma \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Arguing as in A.2.2 we see that

$$n_q(S_{\gamma, 0}, n) = n_q(S_{1, 0}, n) = q^{2n-t-2} \cdot \frac{(q^{n-(t+1)/2} - 1)(q^{n-(t+3)/2} + 1)}{q - 1}.$$

Hence, this case contributes $(q^{2n-t-2}(q^{n-(t+1)/2} - 1)(q^{n-(t+3)/2} + 1))$ to $n_q(S, n)$.

B.3.3) $\boxed{(\gamma, \delta) = (0, 0).}$ We need to compute $n_q(S_{0,0}, n)$, i.e. the number of solutions of the following system in the unknowns $x_{t+2}, \dots, x_{2n+1}, y_{t+2}, \dots, y_{2n+1}$

$$\begin{cases} \mathbf{q}_n(A) + 0x_{t+2} + x_{t+3}x_{t+4} + \dots + x_{2n}x_{2n+1} = 0 \\ 0y_{t+2} + y_{t+3}y_{t+4} + \dots + y_{2n}y_{2n+1} = 0 \\ 0y_{t+2} + x_{t+2}0 + x_{t+3}y_{t+4} + x_{t+4}y_{t+3} + \dots + x_{2n+1}y_{2n} = 0. \end{cases} \quad (11)$$

We shall refer to the system in the unknowns $x_{t+3}, \dots, x_{2n+1}, y_{t+3}, \dots, y_{2n+1}$ obtained from (11) by removing the unknowns x_{t+2} and y_{t+2} as the “reduced” system. With arguments similar to those of A.3.2) we see that each solution of the reduced system corresponds to q^2 solutions of (11). However, there are also solutions of (11) not arising from the reduced system. These solutions correspond to cases in which $y_{t+2} \neq 0$ and $y_{t+3} = \dots = y_{2n+1} = 0$; that is, they are of the form

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t & 0 & 0 & x_{t+3} & \dots & x_{2n+1} \\ 0 & 0 & \dots & 0 & 0 & 1 & 0 & \dots & 0 \end{pmatrix}$$

and they number in $\eta_1(\mathfrak{q}_n(A))$; see (9). Hence,

$$n_q(S_{0,0}, n) = q^2 n_q(S, n-1) + \eta_1(\mathfrak{q}_n(A)).$$

The case $A = \mathbf{0}$ and $B \neq \mathbf{0}$ cannot happen according to the convention we adopted.

The above arguments provide a complete description of how to compute the function $n_q(S, n)$ for any $S \in \mathcal{M}_2^1$ and $n \in \mathbb{N}$.

We summarize the details of the algorithm in Table 4.

2.2.3 Complexity

We now analyze the complexity of the algorithm described in sections 2.2.1 and 2.2.2. Given a $2 \times t$ matrix $S = \begin{pmatrix} A \\ B \end{pmatrix}$ in RREF and $n \in \mathbb{N}$, we shall denote by $n_q^E(S, n)$ the output of the algorithm with t even (see Section 2.2.1) and by $n_q^O(S, n)$ the output with t odd (see Section 2.2.2). We will write $\kappa(n_q(S, n))$ for the number of operations required to compute $n_q(S, n)$. The complexity of the various steps of the algorithm are now examined.

STEP 1. If $S = \emptyset$ or we are in the hypotheses of case A.2.2, A.3.1 or B.2, then we can provide the value of $n_q(S, n)$ by directly applying a formula with complexity $O(1)$; see also Table 4.

STEP 2. Otherwise, transform S in CRREF; this requires at most t products and t sums.

STEP 3. If t is even, compute $n_q^E(S, n)$; otherwise compute $n_q^O(S, n)$.

Clearly,

$$\kappa(n_q(S, n)) \leq t + \max\{\kappa(n_q^E(S, n)), \kappa(n_q^O(S, n))\}.$$

We shall now analyze in detail $\kappa(n_q^E(S, n))$ and $\kappa(n_q^O(S, n))$.

- $n_q^E(S, n)$.

1. If S satisfies the hypotheses of A.1, then we need to evaluate $\mathfrak{q}_n(A)$; this requires t products and t sums; thus it has complexity $O(t)$. Likewise, also under the assumptions of A.2.1, determining $n_q(S, n)$ has complexity $O(t)$.
2. If S satisfies the hypotheses of A.3.2 or A.3.3, we need to consider the complexity of $n_q^O(S', n-1)$ where S' is a $2 \times (t-1)$ matrix obtained from S by deleting its last column. Then we need to consider a case odd length $n_q^O(S', n-1)$. As it will be shown below, the complexity here is at most $O(n^2)$.

- $n_q^O(S, n)$. We claim that

$$\kappa(n_q^O(S, n)) \leq 3t + \kappa(n_q^O(S, n-1)). \quad (12)$$

Table 4: Enumerator for Orthogonal Line Grassmannians

$S = \begin{pmatrix} A \\ B \end{pmatrix}$	t	Case	$n_{\mathbf{q}}(S, n)$	Complexity
\emptyset	0		N	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & \beta_t \end{pmatrix}$ $\beta_t \neq 0$	Even	A.1	$q^{2n-t}\eta_0(\mathbf{q}_n(A))$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & 0 \end{pmatrix}$ $\alpha_t \neq 0$ $(\beta_1, \dots, \beta_{t-1}) \neq \mathbf{0}$	Even	A.2.1	$q^{2n-t}\eta_0(\mathbf{q}_n(B))$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $\alpha_t \neq 0$	Even	A.2.2	$\frac{q^{2n-t-1}}{q-1}(q^{n-t/2} - 1)(q^{n-t/2-1} + 1)$	$O(1)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Even	A.3.1	$\sigma q^2 + (q^{n-t/2} - 1)(q^{n-t/2-1} + 1)$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}) \neq \mathbf{0}$	Even	A.3.2	$q^2 n_{\mathbf{q}}(S', n-1) + \eta_0(\mathbf{q}_n(A))$	$O(n^2)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_{t-1}) \neq \mathbf{0}$	Even	A.3.3	$q^2 n_{\mathbf{q}}(S', n-1)$	$O(n^2)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}, \alpha_t) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_{t-1}, \beta_t) \neq \mathbf{0}$	Odd	B.1	$\Psi_{\substack{\gamma \neq 0 \\ \delta \neq 0}} + \Psi_{\substack{\gamma \neq 0 \\ \delta = 0}} + \Psi_{\substack{\gamma = 0 \\ \delta \neq 0}} + \Psi_{\substack{\gamma = 0 \\ \delta = 0}}$	$O(n^2)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Odd	B.2	$\frac{(q^{2n-t-1}-1)(q^{n-(t-1)/2}-1)(q^{n-(t-3)/2}+1)}{(q^2-1)(q-1)}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ 0 & 0 & \dots & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$	Odd	B.3	$n_{\mathbf{q}}(S_{0,1}, n) + n_{\mathbf{q}}(S_{1,0}, n) + n_{\mathbf{q}}(S_{0,0}, n)$	$O(n^2)$

For the meaning of the symbols and the constants, see the relevant sections.

By B.1 and B.3 computing $n_q^O(S, n)$ requires to determine the values of $n_q^E(S_{\gamma, \delta}, n)$ for $(\gamma, \delta) = (0, 1)$, $(\gamma, \delta) = (1, 0)$ and $\gamma \neq 0 \neq \delta$ and also of $n_q^O(S, n-1)$. The first three cases have already been shown to have complexity at most $O(t)$. Hence, the claim follows.

Observe that $\kappa(n_q^O(S, \frac{t-1}{2})) = 3^{\frac{t-1}{2}}$, since, in this case, we just need to check if the line spanned by A and B is totally singular. Note that $n_q^O(S, \frac{t-1}{2})$ is the number totally singular lines of $\text{PG}(t-1, q)$ having the prefix S of length t . Clearly, this number is 1 if the line spanned by the rows of S is singular and 0 otherwise. By recursively applying (12), since $t \leq 2n+1$, we have

$$\begin{aligned} \kappa(n_q^O(S, n)) &\leq 3t + \kappa(n_q^O(S, n-1)) + O(1) \leq 6t + \kappa(n_q^O(S, n-2)) + O(1) \leq \dots \\ &\leq 3 \sum_{i=1}^{n-(t+1)/2} t + \kappa(n_q^O(S, \frac{t-1}{2})) + O(1) \leq O(n^2). \end{aligned}$$

In summary, the complexity of the algorithm to determine $n_q(S, n)$ is $O(n^2)$.

2.3 Symplectic Grassmannians

Following Definition 1, for any $S = \begin{pmatrix} A \\ B \end{pmatrix} \in \mathcal{M}_2^0$, where $A = (\alpha_1, \dots, \alpha_t, 0, \dots, 0)$, $B = (\beta_1, \dots, \beta_t, 0, \dots, 0)$, denote by $n_s(S, n)$ the number of totally \mathfrak{s} -isotropic lines of $\text{PG}(2n-1, q)$ spanned by $\hat{A} = (\alpha_1, \dots, \alpha_t, x_{t+1}, \dots, x_{2n})$ and $\hat{B} = (\beta_1, \dots, \beta_t, y_{t+1}, \dots, y_{2n})$. Recall that $\begin{pmatrix} \hat{A} \\ \hat{B} \end{pmatrix}$ is in RREF. In this section, with an approach similar to that of Section 2.2, we compute $n_s(S, n)$. Equivalently, we have to study the solutions of the equation $\mathfrak{s}(\hat{A}, \hat{B}) = 0$, see (2) in the unknowns $x_{t+1}, \dots, x_{2n}, y_{t+1}, \dots, y_{2n}$. The first step of the algorithm is to transform S in CRREF using (3).

Let \mathfrak{s}' be the alternating form induced by the restriction of S on the subspace of \bar{V} of equation $x_1 = x_2 = \dots = x_t = 0$.

We distinguish two subcases.

2.3.1 Even t

There are three possibilities:

C.1) $\boxed{A = B = \mathbf{0}}$. In this case, $n_s(S, n)$ is the number of totally isotropic lines for \mathfrak{s}' in a $\text{PG}(2n-t-1, q)$. Thus,

$$n_s(S, n) = \frac{(q^{2n-t} - 1)(q^{2n-t-2} - 1)}{(q-1)(q^2 - 1)}.$$

C.2) $\boxed{A \neq \mathbf{0}, B = \mathbf{0}}$. In this case, we have

$$G = \begin{pmatrix} \alpha_1 & \dots & \alpha_t & x_{t+1} & \dots & x_{2n} \\ 0 & \dots & 0 & y_{t+1} & \dots & y_{2n} \end{pmatrix}.$$

Suppose $Y = (y_{t+1}, \dots, y_{2n})$ is a given non-null vector with leading coefficient $y_i = 1$, $i > t$. There are $\frac{q^{2n-t}-1}{q-1}$ choices for Y . For any such Y we count the number of vectors $X = (x_{t+1}, \dots, x_{2n})$ with $x_i = 0$ such that $\mathfrak{s}'(X, Y) = 0$. This amounts to q^{2n-t-2} choices for X . Hence,

$$n_s(S, n) = q^{2n-t-2} \frac{q^{2n-t} - 1}{q - 1}.$$

C.3) $A \neq \mathbf{0}, B \neq \mathbf{0}$. We distinguish two subcases, according to the value of $\mathfrak{s}(A, B)$.

C.3.1) $\mathfrak{s}(A, B) = 0$: in this case we count the number of pairs of vectors (X, Y) with $X, Y \in \mathbb{F}_q^{2n-t}$ and $\mathfrak{s}(X, Y) = 0$. If $X = \mathbf{0}$, then there are q^{2n-t} different choices for Y such that $\mathfrak{s}'(X, Y) = 0$. If $X \neq \mathbf{0}$, there are q^{2n-t-1} choices for Y such that $\mathfrak{s}'(X, Y) = 0$. Thus,

$$n_{\mathfrak{s}}(S, n) = q^{2n-t-1}(q^{2n-t} - 1) + q^{2n-t}. \quad (13)$$

C.3.2) $\mathfrak{s}(A, B) \neq 0$: Let $X = (x_{t+1}, \dots, x_{2n})$ be a fixed non-null vector. There are $q^{2n-t}-1$ choices for such X . We count the number of vectors $Y = (y_{t+1}, \dots, y_{2n})$ such that $\mathfrak{s}'(X, Y) = -\mathfrak{s}(A, B)$. This is a linear equation in the unknowns y_{t+1}, \dots, y_{2n} ; hence, there are q^{2n-t-1} choices for Y . Thus,

$$n_{\mathfrak{s}} = (q^{2n-t} - 1)q^{2n-t-1}. \quad (14)$$

2.3.2 Odd t

When t is odd, the technique we apply to determine $n_{\mathfrak{s}}(S, n)$ is to replace $S := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$, with a larger matrix $S_{\gamma, \delta} := \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t & \gamma \\ \beta_1 & \beta_2 & \dots & \beta_t & \delta \end{pmatrix}$ in CRREF obtained from S by adding the column $\begin{pmatrix} \gamma \\ \delta \end{pmatrix}$.

We distinguish three cases

D.1) $A = B = \mathbf{0}$. In this case, the only two matrices $S_{\gamma, \delta}$ which are in CRREF are $S_{0,0}$ and $S_{1,0}$. Thus,

$$n_{\mathfrak{s}}(S, n) = n_{\mathfrak{s}}(S_{0,0}, n) + n_{\mathfrak{s}}(S_{1,0}, n)$$

where $n_{\mathfrak{s}}(S_{0,0}, n)$ and $n_{\mathfrak{s}}(S_{1,0}, n)$ are computed as in C.1) and C.2) of Section 2.3.1.

D.2) $A \neq \mathbf{0}, B = \mathbf{0}$. In this case, the only matrices $S_{\gamma, \delta}$ in CRREF are $S_{\gamma,0}$ with $\gamma \in \mathbb{F}_q$ and $S_{0,1}$. Thus,

$$n_{\mathfrak{s}}(S, n) = \sum_{\gamma \in \mathbb{F}_q} n_{\mathfrak{s}}(S_{\gamma,0}, n) + n_{\mathfrak{s}}(S_{0,1}, n).$$

By Case C.2) of Section 2.3.1, $n_{\mathfrak{s}}(S_{\gamma,0}, n) = n_{\mathfrak{s}}(S_{0,0}, n)$ for all $\gamma \in \mathbb{F}_q$; thus

$$n_{\mathfrak{s}}(S, n) = qn_{\mathfrak{s}}(S_{0,0}, n) + n_{\mathfrak{s}}(S_{0,1}, n)$$

where $n_{\mathfrak{s}}(S_{0,1}, n)$ is computed in Case C.3) of Section 2.3.1 (and $n_{\mathfrak{s}}(S_{0,0}, n)$ is computed in Case C.2)).

D.3) $A \neq \mathbf{0}, B \neq \mathbf{0}$. There are two possibilities.

D.3.1) $\alpha_t = \beta_t = 0$. In this case, we have to consider

$$S_{\gamma, \delta} = \begin{pmatrix} \alpha_1 & \dots & \alpha_{t-1} & 0 & \gamma \\ \beta_1 & \dots & \beta_{t-1} & 0 & \delta \end{pmatrix}.$$

Observe that the value of $n_s(S_{\gamma,\delta}, n)$ corresponds to either case C.3.1) or C.3.2) of Section 2.3.1 according as $\mathfrak{s}(A, B) = 0$ or $\mathfrak{s}(A, B) \neq 0$ but does not depend on the choice of γ and δ . Thus,

$$n_s(S, n) = q^2 n_s(S_{0,0}, n).$$

D.3.2) $\boxed{(\alpha_t, \beta_t) \neq (0, 0)}$. Let $A_\gamma = (\alpha_1, \dots, \alpha_t, \gamma, 0, \dots, 0)$ and $B_\delta = (\beta_1, \dots, \beta_t, \delta, 0, \dots, 0)$. Clearly,

$$\mathfrak{s}(A_\gamma, B_\delta) = \alpha_1 \beta_2 - \alpha_2 \beta_1 + \dots + \alpha_t \delta - \beta_t \gamma.$$

As (α_i, β_i) for $i = 1, \dots, t$ are all given and $(\alpha_t, \beta_t) \neq (0, 0)$, $\mathfrak{s}(A_\gamma, B_\delta) = 0$ is a non-trivial linear equation in the unknowns γ and δ . Hence, there are exactly q values of (γ, δ) such that $\mathfrak{s}(A_\gamma, B_\delta) = 0$. For each of these values we have by Case C.3.1) $q^{2n-t-2}(q^{2n-t-1} - 1) + q^{2n-t-1}$ distinct lines to take into account. For the remaining $q^2 - q$ values of (γ, δ) such that $\mathfrak{s}(A_\gamma, B_\delta) \neq 0$ we have, by Case C.3.2) $(q^{2n-t-1} - 1) \frac{q^{2n-t-1} - q^{2n-t-2}}{q-1}$ distinct lines. Consequently,

$$n_s(S, n) = q^{4n-2t-1}.$$

2.3.3 Complexity

The computational complexity of the algorithm to compute $n_s(S, n)$ for a given S in RREF and $n \in \mathbb{N}$ is $O(n)$. This can be immediately seen by analyzing the steps of the algorithm described in the previous sections. For the convenience of the reader we summarize the various cases, depending on the structure of S , together with their complexity, in Table 5.

3 Enumerative coding

In this section, following the approach of [7], we construct enumerators for the points of $\Delta_{n,k}$ and $\bar{\Delta}_{n,k}$ using the functions n_q and n_s introduced before. We shall present the full details for the orthogonal Grassmannian $\Delta_{n,2}$; the symplectic case is entirely analogous.

Fix a total order \preceq on the vectors of \mathbb{F}_q^2 and write $A \prec B$ if and only if $A \preceq B$ and $A \neq B$. Let ℓ be a totally \mathfrak{q} -singular line of V and $G_\ell = (G_1, \dots, G_{2n+1})$ be its representation (in RREF), where $G_i \in \mathbb{F}_q^2$ is the i -th column of G_ℓ . For any $j \leq 2n+1$ and $X \in \mathbb{F}_q^2$, let $S_j^X := (G_1, \dots, G_{j-1}, X)$ be the $(2 \times j)$ -matrix comprising the first $j-1$ columns of G_ℓ and whose last column is X .

Let $\mathbb{I} = \{0, \dots, N-1\}$, with $N = \#\Delta_{n,2}$, see Table 1 and define

$$\iota : \begin{cases} \Delta_{n,2} \rightarrow \mathbb{I} \\ \ell \mapsto \iota(G_\ell) := \sum_{j=1}^{2n+1} \sum_{X \prec G_j} n_q(S_j^X, n). \end{cases} \quad (15)$$

We remark that the order \prec defined on the vectors of \mathbb{F}_q^2 can be extended to matrices of order $2 \times (2n+1)$ lexicographically, that is $G \ll H$ if and only if there exists $i \in \{1, \dots, 2n+1\}$ such that $\forall j < i$ $G_j = H_j$ and $G_i \prec H_i$. It will be natural to see that $G \ll H$ if and only if $\iota(G) < \iota(H)$.

We say that a vector $X \in \mathbb{F}_q^2$ is *allowable in position j for (G_1, \dots, G_{j-1})* if and only if $n_q(S_j^X, n) > 0$, that is to say, $(G_1, \dots, G_{j-1}, X, X_{j+1}, \dots, X_{2n+1})$ represents a totally \mathfrak{q} -singular line for at least one choice of X_{j+1}, \dots, X_{2n+1} .

Table 5: Enumerator for Symplectic Line Grassmannians

$S = \begin{pmatrix} A \\ B \end{pmatrix}$	t	Case	$n_{\mathfrak{s}}(S, n)$	Complexity
\emptyset	0		N	$O(1)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Even	C.1	$q^{2n-t-2} \frac{q^{2n-t}-1}{q-1}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$	Even	C.2	$q^{2n-t-2} \frac{q^{2n-t}-1}{q-1}$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_t) \neq \mathbf{0}$ $\mathfrak{s}(A, B) = 0$	Even	C.3.1	$q^{2n-t-1}(q^{2n-t} - 1) + q^{2n-t}$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_t) \neq \mathbf{0}$ $\mathfrak{s}(A, B) \neq 0$	Even	C.3.2	$(q^{2n-t} - 1)q^{2n-t-1}$	$O(t)$
$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$	Odd	D.1	$n_{\mathfrak{s}}(S_{0,0}, n) + n_{\mathfrak{s}}(S_{1,0}, n)$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & \alpha_t \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_t) \neq \mathbf{0}$	Odd	D.2	$qn_{\mathfrak{s}}(S_{0,0}, n) + n_{\mathfrak{s}}(S_{0,1}, n)$	$O(1)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{t-1} & 0 \\ \beta_1 & \beta_2 & \dots & \beta_{t-1} & 0 \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_{t-1}) \neq \mathbf{0}$	Odd	D.3.1	$q^2 n_{\mathfrak{s}}(S_{0,0}, n)$	$O(t)$
$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \beta_1 & \beta_2 & \dots & \beta_t \end{pmatrix}$ $(\alpha_1, \dots, \alpha_{t-1}) \neq \mathbf{0}$ $(\beta_1, \dots, \beta_{t-1}) \neq \mathbf{0}$ $(\alpha_t, \beta_t) \neq (0, 0)$	Odd	D.3.2	$q^{4n-2t-1}$	$O(1)$

Theorem 6. *The index function ι defined in (15) is a bijection.*

Proof. As $\#\Delta_{n,2} = \#\mathbb{I}$, it is enough to show that ι is injective. Let

$$\begin{aligned} G &= (H_1, H_2, \dots, H_{i-1}, G_i, \dots, G_{2n+1}); \\ H &= (H_1, H_2, \dots, H_{i-1}, H_i, \dots, H_{2n+1}). \end{aligned}$$

We will show that if $G_i \prec H_i$, then $\iota(G) < \iota(H)$. In this case, $G \ll H$. Suppose $G_i \prec H_i$ and define

$$\begin{aligned} \iota^\prec(G) &:= \{(X_1, \dots, X_{2n+1}) : X_1 \prec G_1\} \cup \{(G_1, X_2, \dots, X_{2n+1}) : X_2 \prec G_2\} \cup \dots \\ &\dots \cup \{(G_1, G_2, \dots, G_{2n}, X_{2n+1}) : X_{2n+1} \prec G_{2n+1}\}, \end{aligned} \quad (16)$$

where the elements of the various sets all are matrices in RREF representing totally singular lines. Clearly, if $G_1 = H_1, \dots, G_{i-1} = H_{i-1}$ and $G_i \prec H_i$ for some columns H_1, \dots, H_i , then

$$G \in \{(G_1, \dots, G_{i-1}, X_i, X_{i+1}, \dots, X_{2n+1}) : X_i \prec H_i\};$$

in particular, $G \in \iota^\prec(H)$. Furthermore, if $G \in \iota^\prec(H)$, then $\iota^\prec(G) \subset \iota^\prec(H)$. By hypothesis, there exists i such that for all $s < i$, $H_s = G_s$ and $G_i \prec H_i$. Suppose $Y := (Y_1, \dots, Y_{2n+1}) \in \iota^\prec(G)$. Then, there exists j such that $Y_1 = G_1, \dots, Y_{j-1} = G_{j-1}$ and $Y_j \prec G_j$; in particular,

- If $j < i$, then $Y_1 = G_1 = H_1, \dots, Y_{j-1} = G_{j-1} = H_{j-1}$ and $Y_j \prec H_j = G_j$; thus $Y \in \iota^\prec(H)$.
- If $j = i$, then $Y_i \prec G_i \prec H_i$ and $Y \in \{(G_1, \dots, G_{i-1}, X_i, X_{i+1}, \dots, X_{2n+1}) : X_i \prec H_i\}$; thus $Y \in \iota^\prec(H)$.
- If $j > i$, then $Y_i = G_i \prec H_i$; thus,

$$Y \in \{(G_1, \dots, G_{i-1}, X_i, X_{i+1}, \dots, X_{2n+1}) : X_i \prec H_i\};$$

consequently, $Y \in \iota^\prec(H)$.

As $G \in \iota^\prec(H)$ but $G \notin \iota^\prec(G)$, the above inclusions are proper. We now show that $\iota(G) = \#\iota^\prec(G)$. Note that

$$\begin{aligned} \#\{(G_1, G_2, \dots, G_{i-1}, X_i, X_{i+1}, \dots, X_{2n+1}) : X_i \prec G_i\} &= \\ \sum_{X_i \prec G_i} \#\{(G_1, G_2, \dots, G_{i-1}, X_i, X_{i+1}, \dots, X_{2n+1})\} &= \sum_{X_i \prec G_i} n_q((G_1, \dots, G_{i-1}, X_i), n). \end{aligned}$$

Furthermore, as the sets in (16) are disjoint,

$$\begin{aligned} \#\iota^\prec(G) &= \#\{(X_1, \dots, X_{2n+1}) : X_1 \prec G_1\} + \#\{(G_1, X_2, \dots, X_{2n+1}) : X_2 \prec G_2\} + \dots \\ &\quad + \#\{(G_1, G_2, \dots, G_{2n}, X_{2n+1}) : X_{2n+1} \prec G_{2n+1}\} = \\ \sum_{X_1 \prec G_1} n_q((X_1), n) &+ \sum_{X_2 \prec G_2} n_q((G_1 \ X_2), n) + \dots + \sum_{X_{2n+1} \prec G_{2n+1}} n_q((G_1 \ G_2 \ \dots \ G_{2n} \ X_{2n+1}), n) = \\ &= \sum_{i=1}^{2n+1} \sum_{X_i \prec G_i} n_q((G_1, \dots, G_{i-1}, X_i), n) = \iota(G). \end{aligned}$$

To conclude, observe that for any two distinct lines represented by matrices G and H in RREF we have either $G \in \iota^\prec(H)$ or $H \in \iota^\prec(G)$. The former yields $\iota^\prec(G) \subset \iota^\prec(H)$, whence $\iota(G) < \iota(H)$; the latter, in an entirely analogous way, $\iota(G) > \iota(H)$. In any case $G \neq H$ gives $\iota(G) \neq \iota(H)$ and ι is injective. \square

In the following theorem we show how to construct the columns of the representative matrix G_ℓ of a line ℓ given an index $i \in \mathbb{I}$. Each column G_s of G_ℓ is shown to be the maximum allowable vector of \mathbb{F}_q^2 for the given value of i .

Theorem 7. Suppose $G = (G_1, \dots, G_{2n+1})$ represents a totally singular line ℓ and let $\iota(G) = i$. Let also for any $k = 1 \dots 2n+1$,

$$\theta(G_{\leq k}) := \sum_{X \prec G_k} n_q(S_k^X, n), \quad i_k := i - \sum_{j=1}^{k-1} \theta(G_{\leq j}).$$

Then, G_k is the maximum allowable column of G with respect to the order \prec such that $\theta(G_k) \leq i_k$.

Proof. Define

$$\begin{aligned} \Theta(G_{\leq k}) &:= \{(G_1, \dots, G_{k-1}, X, \dots) : X \prec G_k\}, \\ \Lambda(G_{\leq k}) &:= \{(G_1, \dots, G_{k-1}, Y, \dots) \in \iota^\prec(G) : Y \preceq G_k\}. \end{aligned}$$

Then,

$$\Lambda(G_{\leq 1}) = \{(Y, \dots) \in \iota^\prec(G) : Y \preceq G_1\} = \iota^\prec(G).$$

We have

$$\#\Theta(G_{\leq k}) = \sum_{X \prec G_k} n_q(S_k^X, n) = \theta(G_{\leq k}).$$

On the other hand, for $k > 1$ we can write

$$\begin{aligned} \Lambda(G_{\leq k}) &= \iota^\prec(G) \setminus \left(\{(X_1, \dots) : X_1 \prec G_1\} \cup \{(G_1, X_2, \dots) : X_2 \prec G_2\} \cup \dots \right. \\ &\quad \left. \dots \cup \{(G_1, G_2, \dots, G_{k-2}, X_{k-1}, \dots) : X_{k-1} \prec G_{k-1}\} \right) = \iota^\prec(G) \setminus \bigcup_{j=1}^{k-1} \Theta(G_{\leq j}). \end{aligned}$$

Thus,

$$\#\Lambda(G_{\leq k}) = \iota(G) - \sum_{j=1}^{k-1} \theta(G_{\leq j}) = i_k.$$

We distinguish two cases:

- $k = 1$. By way of contradiction, suppose G_1 is not maximum and $\theta(G_{\leq 1}) \leq i_1 = i$. Then, there is an element $G'_1 \in \mathbb{F}_q^2$, with $G_1 \prec G'_1$ and $\theta(G'_{\leq 1}) \leq i$. By construction, $\Lambda(G_{\leq 1}) \subset \Theta(G'_{\leq 1})$. Observe that $G \in \Theta(G'_{\leq 1})$ but $G \notin \Lambda(G_{\leq 1})$. Thus, the inclusion is proper. Moving to the cardinalities we have

$$i = \#\Lambda(G_{\leq 1}) < \#\Theta(G'_{\leq 1}) = \theta(G'_{\leq 1}) \leq i,$$

a contradiction.

- $k > 1$. Suppose that the thesis holds for $j \leq k$ but not for $j = k+1$ i.e. all G_j 's for $j \leq k$ are maximum and $\theta(G_{\leq j}) \leq i_j$ and G_{k+1} is not the maximum element such that $\theta(G_{\leq k+1}) \leq i_{k+1}$. Then, as before, there is a G'_{k+1} such that $G_{k+1} \prec G'_{k+1}$ with $\theta(G'_{\leq k+1}) \leq i_{k+1}$. For any $Y \preceq G_{k+1}$ we have $Y \prec G'_{k+1}$; thus, the following holds

$$\begin{aligned} \Lambda(G_{\leq k+1}) &= \{(G_1, \dots, G_k, Y, \dots) \in \iota^\prec(G) : Y \preceq G_{k+1}\} \subset \\ &\subset \{(G_1, \dots, G_k, X, \dots) : X \prec G'_{k+1}\} = \Theta(G'_{\leq k+1}). \end{aligned}$$

Furthermore, as $G \in \Theta(G'_{\leq k+1})$ but $G \notin \Lambda(G_{\leq k+1})$, the above inclusion is proper. Thus,

$$i_{k+1} = \#\Lambda(G_{\leq k+1}) < \#\Theta(G'_{\leq k+1}) = \theta(G'_{\leq k+1}) \leq i_{k+1},$$

a contradiction. □

In Table 6 we show in detail the procedure arising from Theorem 7 to efficiently invert the function ι . Observe that the check $n_q((G_1, \dots, G_k), n) > 0$ is necessary, as each column G_k must

Require: $i \in \{0, \dots, N-1\}$
 $i_1 \leftarrow 1$
for $k = 1, \dots, 2n+1$ **do**
 $M \leftarrow \{Y : \sum_{X \prec Y} n_q(S_k^X, n) \leq i_k \text{ and } n_q(S_k^Y, n) > 0\}$
 $G_k \leftarrow \max M$
 $\theta(G_k) \leftarrow \sum_{X \prec G_k} n_q(S_k^X, n);$
 $i_{k+1} \leftarrow i_k - \theta(G_{\leq k});$
end for
return $G = (G_1, \dots, G_k, \dots, G_{2n+1})$

Table 6: Inverse of ι

be allowable and columns which are allowable in a given position k may not be allowable in position $k-1$ or *vice-versa*.

3.1 Complexity

We now estimate the actual cost of the enumerative encoding presented in this section. In the orthogonal case, to evaluate ι we need to compute at most $q^2 - 1$ values of $n_q(S_j^X, n)$ for any $j = 1, \dots, 2n+1$ as X varies in \mathbb{F}_q^2 . So, the overall complexity turns out to be $O(q^2 n^3)$. Conversely, given an index $i \in \mathbb{I}$, recovering the corresponding line $\ell = \iota^{-1}(i)$ requires to test at most $q^2 - 1$ vectors $X \in \mathbb{F}_q^2$ for each column of G ; thus, the cost is once more $O(q^2 n^3)$. In the symplectic case, the same arguments give a complexity of $O(q^2 n^2)$ for enumerative encoding.

4 Application to orthogonal polar Grassmann codes

We now apply the enumeration techniques discussed in the previous sections to efficiently implement the orthogonal linear codes $\mathcal{P}_{n,2}$.

4.1 Encoding

As in Section 2.2, let V be a vector space of dimension $2n+1$ over \mathbb{F}_q and fix a basis $\mathfrak{B} := (\mathbf{e}_1, \dots, \mathbf{e}_{2n+1})$ of V .

It is well known that the dual $(\bigwedge^k V)^*$ of the vector space $\bigwedge^k V$ is isomorphic to $\bigwedge^{2n+1-k} V$. We recall the following universal property of the k^{th} -exterior power of a vector space.

Theorem 8 [22, Theorem 14.23]. *Let V, U be two vector spaces over the same field. A map $f : V^k \rightarrow U$ is alternating k -linear if, and only if, there is a linear map $\bar{f} : \bigwedge^k V \rightarrow U$ with $\bar{f}(v_1 \wedge v_2 \wedge \dots \wedge v_k) = f(v_1, v_2, \dots, v_k)$. The map \bar{f} is uniquely determined.*

For $k = 2$, any linear functional on $\bigwedge^2 V$ corresponds to a bilinear alternating form on V , hence it can be represented by an antisymmetric matrix M .

By Theorem 8, each $\zeta \in (\bigwedge^2 V)^*$ is represented with respect to \mathfrak{B} by a $(2n+1) \times (2n+1)$ antisymmetric matrix M whose entries are $m_{i,j} = \zeta(\mathbf{e}_i \wedge \mathbf{e}_j)$.

As vector spaces, the codes $\mathcal{P}_{n,2}$ are isomorphic to quotients $(\bigwedge^2 V)^*/W$ where W consists of all elements $f : \bigwedge^2 V \rightarrow \mathbb{F}_q$ which are identically zero respectively on $\varepsilon_2(\Delta_{n,2})$ and $\varepsilon_2(\overline{\Delta}_{n,2})$.

Suppose first q is odd. Then $\dim \mathcal{P}_{n,2} = \dim \langle \varepsilon_2(\Delta_{n,2}) \rangle = \binom{2n+1}{2} = \dim \bigwedge^2 V$; thus, in this case, $W = \{0\}$ and $\mathcal{P}_{n,2}$ is isomorphic as vector space to $(\bigwedge^2 V)^*$.

The encoding technique we propose works as follows.

Take a message $\mathbf{m} \in \bigwedge^2 V$. Suppose $\mathbf{m} = (m_1, \dots, m_{n(2n+1)})$. Consider the antisymmetric matrix $\mathfrak{M} = \mathfrak{M}_0 - \mathfrak{M}_0^T$ where

$$\mathfrak{M}_0 = \begin{pmatrix} 0 & m_1 & m_2 & \dots & m_{2n} \\ 0 & 0 & m_{2n+1} & \dots & m_{4n-1} \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & m_{n(2n+1)} \\ 0 & \dots & \dots & 0 & 0 \end{pmatrix}.$$

Clearly, \mathfrak{M} defines an alternating form $\zeta_M : V \times V \rightarrow \mathbb{F}_q$ with $\zeta(x, y) := x^T \mathfrak{M} y$. Denote by \mathbf{m}_{ij} the entry of M in position (i, j) , with $i < j$. Then, a straightforward counting argument shows that

$$\mathbf{m}_{ij} = m_{2n(i-1)+j-\frac{i^2-i}{2}-1}. \quad (17)$$

If q is even then $\dim \mathcal{P}_{n,2} = \dim \langle \varepsilon_2(\overline{\Delta}_{n,2}) \rangle = \binom{2n+1}{2} - 1 < \dim \bigwedge^2 V$, i.e. W is a proper subspace of $(\bigwedge^2 V)^*$. Let $(e_i)_{i=1}^K$ be a basis of a complement of W in $(\bigwedge^2 V)^*$ and define $\mathfrak{M} = \sum_{i=1}^K m_i e_i$.

Then we encode the message m in the codeword $\mathbf{c} = (c_1, \dots, c_N) \in \mathcal{P}_{n,2}$ where the coordinate c_i , $1 \leq i \leq N$, is obtained by first recovering the line $\ell_i := \iota^{-1}(i) = \langle G_1^{(i)}, G_2^{(i)} \rangle$ having $G_1^{(i)}$ and $G_2^{(i)}$ as vector representatives and then defining

$$c_i := G_1^{(i)T} \mathfrak{M} G_2^{(i)}.$$

It is thus possible to directly encode each component of \mathbf{c} using just \mathbf{m} and without having to resort to the whole generator matrix of the code.

4.2 Decoding

Suppose now that \mathbf{c} is a received codeword. We address now the problem to recover the original message \mathbf{m} . Equivalently, we need to reconstruct the antisymmetric matrix M associated to m . In general, polar Grassmann codes are not systematic, nor there are entries in a codeword corresponding exactly to the values m_{ij} of the message \mathbf{m} .

However, it is possible to provide a list of lines yielding information positions in \mathbf{c} such that the values m_{ij} can be straightforward recovered.

Theorem 9. *Let \mathbf{c} be a received codeword and $\mathfrak{M} = (\mathbf{m}_{ij})_{1 \leq i, j \leq 2n+1}$ be the antisymmetric matrix associated to \mathbf{c} . Suppose the pair (i, j) with $1 \leq i < j \leq 2n+1$ is in one of the following types:*

Type I: $i \geq 2$ even and $j \geq i+2$ or i is odd and $j \geq i+1$;

Type II: $i \geq 2$ even and $j = i+1$;

Type III: $i = 1$. Then the following holds.

If (i, j) is of Type I then $\mathbf{m}_{ij} = c_{\ell_{i,j}}$ where $\ell_{i,j} := \langle e_i, e_j \rangle$.

If (i, j) is of Type II then \mathbf{m}_{ij} can be obtained by solving a system of 4 equations in 4 unknowns.

If (i, j) is of Type III then \mathbf{m}_{ij} can be obtained by solving a system of 3 equations in 3 unknowns.

Proof. If (i, j) is of Type I then we immediately see that $\mathbf{m}_{ij} = c_{\ell_{i,j}}$ where $\ell_{i,j} := \langle e_i, e_j \rangle$.

If (i, j) is of Type II consider two lines $\ell^1 := \langle e_i + e_{i+3}, e_{i+1} - e_{i+2} \rangle$ and $\ell^2 := \langle e_i - e_{i+3}, e_{i+1} + e_{i+2} \rangle$ and call c_x, c_y the corresponding entries of \mathbf{c} . Then we have

$$\begin{cases} \mathbf{m}_{i,i+1} - \mathbf{m}_{i,i+2} - \mathbf{m}_{i+1,i+3} + \mathbf{m}_{i+2,i+3} = c_x \\ \mathbf{m}_{i,i+1} + \mathbf{m}_{i,i+2} + \mathbf{m}_{i+1,i+3} - \mathbf{m}_{i+2,i+3} = c_y \end{cases}$$

The entries $\mathbf{m}_{i+1,i+3}$ and $\mathbf{m}_{i,i+2}$ correspond to indexes of type I; thus they can be read off \mathbf{c} directly. The remaining unknowns $\mathbf{m}_{i,i+1}$ and $\mathbf{m}_{i+2,i+3}$ can now be recovered by solving a system in two unknowns. Observe that this operation has fixed complexity $O(1)$.

Suppose $(i, j) = (1, j)$ is of Type III. If $j > 3$, we consider the line $\ell = \langle e_1 - e_2 + e_3, e_j \rangle$. A straightforward computation shows that the corresponding entry c_z is

$$c_z = \mathbf{m}_{1j} - \mathbf{m}_{2j} + \mathbf{m}_{3j}$$

and both $(2, j)$ and $(3, j)$ are of type I; thus we have just to solve this equation. As for the coefficients \mathbf{m}_{12} and \mathbf{m}_{13} , we just use the entries corresponding to $\ell^{12} = \langle e_1 - e_4 + e_5, e_2 \rangle$ and $\ell^{13} = \langle e_1 - e_4 + e_5, e_3 \rangle$. \square

Theorem 9 shows that it is possible to extract any component of the message \mathbf{m} from a codeword \mathbf{c} with complexity $O(1)$. As such, the complexity to recover the whole of \mathbf{m} is $O(n^2)$.

4.3 Error correction

Locally decodable codes have received much attention in recent years; see [28, 29] for some surveys. In general, a code is *locally decodable* if it is able to recover a given component m_i of a message \mathbf{m} with probability larger than $1/2$ querying just a fixed number of components r_j of the received vector \mathbf{r} — this, clearly, under the assumption that not too many errors have occurred; see [16].

In this section we shall introduce an algorithm to try to reconstruct a correct information position using only some limited “local” information. Suppose that $\mathbf{r} = (r_i)_{i=1,\dots,N} \in \mathbb{F}_q^N$ is any received vector and fix $1 \leq i < N$. Let now ℓ be the line of $Q(2n, q)$ such that $\iota(G_\ell) = i$. Write

$$\Sigma_i := \{\pi : \ell \subseteq \pi \subseteq Q(2n, q), \dim \pi = 3\}$$

for the set of all totally singular planes containing ℓ (we remark that we always use dimension throughout the paper). It is easy to see that there is a bijection between the elements of Σ_i and the points of a $Q(2n-4, q)$. In particular, $\#\Sigma_i = (q^{2n-4} - 1)/(q - 1)$. In absence of errors, there exists a bilinear alternating form $\tilde{\zeta}$ such that $r_j = \tilde{\zeta}(R_1^{(j)}, R_2^{(j)})$ where $R_1^{(j)}, R_2^{(j)}$ span the line ℓ_j with $\iota(\ell_j) = j$ as j varies in $\mathbb{I} = \{1, \dots, N\}$. In particular, all the bilinear forms $\tilde{\zeta}|_\pi$ induced by $\tilde{\zeta}$ on π , as π varies in Σ_i , have the same value on ℓ . This suggests the following algorithm. Suppose r_i to be a component whose value we want to correct, as to recover the originally transmitted value c_i . Then, proceed as follows:

1. Choose a plane $\pi \in \Sigma_i = \{\pi : \iota^{-1}(i) \subseteq \pi \subseteq Q(2n, q), \dim \pi = 3\}$;

2. For any three distinct lines $p, q, s \in \pi$, $p, q \text{ sneq } \ell$, construct the alternating form $\phi_{p,q}$ defined on π and agreeing with r_{ι_p} and r_{ι_q} on p and q ; this corresponds to a 3×3 antisymmetric matrix. With a slight abuse of notation we shall write $\phi_{p,q}(\ell)$ for the value of the form $\phi_{p,q}(G_1, G_2)$, where G_1 and G_2 are the two rows of the matrix representing the line ℓ in RREF.
3. If $\phi_{p,q}(\ell) = r_i$, then accept the value r_i and write $c_i := r_i$; otherwise, determine a new form $\phi_{p',q'}$ using different lines p' and q' contained in π . This step can be iterated over all of the possible $\binom{q^2+q}{2}$ pairs of lines of π different from ℓ . If there is a clear majority, assign to c_i the value determined by these computations; otherwise discard the plane π and iterate again from 1.

Observe that the above procedure first attempts to reconstruct the form $\zeta_M|_\pi$ on the plane π and, then, evaluates this form on the line corresponding to the component i . If just one plane is being used, then it can correct up to $\lfloor (q^2 + q - 2)/4 \rfloor$ errors. A variant of the algorithm can be obtained by choosing different planes in Σ_i and then, ultimately, assigning to c_i the value the forms computed on most of them agree on.

References

- [1] S. Ball and A. Blokhuis. A bound for the maximum weight of a linear code. *SIAM J. Discrete Math.*, 27(1):575–583, 2013.
- [2] I. Cardinali and L. Giuzzi. Codes and caps from orthogonal Grassmannians. *Finite Fields Appl.*, 24:148–169, 2013.
- [3] I. Cardinali and L. Giuzzi. Minimum distance of symplectic Grassmann codes. *Linear Algebra Appl.*, 488:124–134, 2016.
- [4] I. Cardinali, L. Giuzzi, K. V. Kaipa, and A. Pasini. Line polar grassmann codes of orthogonal type. *J. Pure Appl. Algebra*, 220(5):1924–1934, 2016.
- [5] I. Cardinali, A. Pasini, Line polar grassmann codes of orthogonal type. *J. Algebr. Comb.*, 38:863–888, 2013.
- [6] J. Carrillo-Pacheco and F. Zaldívar. On Lagrangian-Grassmannian codes. *Des. Codes Cryptogr.*, 60(3):291–298, 2011.
- [7] T. M. Cover. Enumerative source encoding. *IEEE Trans. Information Theory*, IT-19(1):73–77, 1973.
- [8] B. De Bruyn, Some subspaces of the k -th exterior power of a symplectic vector space, *Linear Algebra Appl.* 430:3095-3104, 2009.
- [9] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, 2015.
- [10] S. R. Ghorpade and K. V. Kaipa. Automorphism groups of Grassmann codes. *Finite Fields Appl.*, 23:80–102, 2013.
- [11] S. R. Ghorpade and G. Lachaud. Hyperplane sections of Grassmannians and the number of MDS linear codes. *Finite Fields Appl.*, 7(4):468–506, 2001.

- [12] S. R. Ghorpade, A. R. Patil, and H. K. Pillai. Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes. *Finite Fields Appl.*, 15(1):54–68, 2009.
- [13] W. V. D. Hodge and D. Pedoe. *Methods of algebraic geometry. Vol. I.* Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. Book I: Algebraic preliminaries, Book II: Projective space, Reprint of the 1947 original.
- [14] W. V. D. Hodge and D. Pedoe. *Methods of algebraic geometry. Vol. II.* Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. Book III: General theory of algebraic varieties in projective space, Book IV: Quadrics and Grassmann varieties, Reprint of the 1952 original.
- [15] K. V. Kaipa and H. K. Pillai. Weight spectrum of codes associated with the Grassmannian $G(3, 7)$. *IEEE Trans. Inform. Theory*, 59(2):986–993, 2013.
- [16] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 80–86 (electronic). ACM, New York, 2000.
- [17] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.
- [18] J. Limbupasiriporn, L. Storme, and P. Vandendriessche. Large weight code words in projective space codes. *Linear Algebra Appl.*, 437(3):809–816, 2012.
- [19] Y. Medvedeva. Fast enumeration for grassmannian space. In *Problems of Redundancy in Information and Control Systems (RED), 2012 XIII International Symposium on*, pages 48–52. IEEE, 2012.
- [20] D. Y. Nogin. Codes associated to Grassmannians. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 145–154. de Gruyter, Berlin, 1996.
- [21] A.A. Premet, I.D. Suprunenko, The Weyl modules and the irreducible representations of the symplectic group with the fundamental highest weights. *Comm. Algebra* 11:1309-1342, 1983.
- [22] S. Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.
- [23] C. Ryan. An application of Grassmannian varieties to coding theory. *Congr. Numer.*, 57:257–271, 1987. Sixteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1986).
- [24] C. T. Ryan. Projective codes based on Grassmann varieties. *Congr. Numer.*, 57:273–279, 1987. Sixteenth Manitoba conference on numerical mathematics and computing (Winnipeg, Man., 1986).
- [25] C. T. Ryan and K. M. Ryan. The minimum weight of the Grassmann codes $C(k, n)$. *Discrete Appl. Math.*, 28(2):149–156, 1990.
- [26] N. Silberstein and T. Etzion. Enumerative coding for Grassmannian space. *IEEE Trans. Inform. Theory*, 57(1):365–374, 2011.

- [27] M. Tsfasman, S. Vlăduț, and D. Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.
- [28] S. Yekhanin. *Locally decodable codes*. NOW Publishers, 2010.
- [29] S. Yekhanin. *Locally Decodable Codes and Private Information Retrieval Schemes*. Information Security and Cryptography Texts and Monographs. Springer, New York, 2010.